Security Essentials for Fermilab System Administrators

09-Nov-2010

Outline

✦ Why Computer Security
✦ Fermilab Strategy:
  – Integrated Computer Security
  – Defense in Depth
✦ Your role and special responsibilities as a user and system administrator
✦ Other Computing Policy Issues
  – Data backup
  – Incidental use
  – Privacy
  – Offensive material
  – Licensing

Some Definitions & Roles

✦ CSEXEC – Computer Security Executive:
  – Vicky White;

✦ FCSC – Fermilab Computer Security Coordinator:
  – Joe Klemencic;

✦ FCIRT – Fermilab Computer Security Incident Response Team:
  – Mike Diesburg (Head);
  – Keith Chadwick (Deputy Head);
  – Manages Fermilab response to computer security incidents.

✦ CST – Computer Security Team;

✦ GCSC – General Computer Security Coordinator:
  – Each Division/Section or large experiment has a GCSC;
  – Acts as liaison with the Computer Security Team in disseminating information and dealing with incidents.

Why Computer Security

✦ The Internet is a dangerous place:
  – We are constantly being scanned for weak or vulnerable systems; new unpatched systems will be exploited within minutes.

✦ Fermilab is an attractive target:
  – High network bandwidth is useful for attackers who take over lab computers;
  – Publicity value of compromising a ".gov" site;
  – Attackers may not realize we have no information useful to them.

Why Computer Security - 2

✦ We need to protect:
  – Our data;
  – Our ability to use our computers (denial of service attacks);
  – Our reputation with DOE, Congress and the general public.

✦ Major sources of danger:
  – Running malicious code on your machine due to system or application vulnerabilities or improper user actions;
    • Responding to email phishing;
    • "Drive by" web infections.
  – Carrying infected machines (laptops) in from off site.

Recent Incidents - Windows

✦ Viruses/Malware arriving via a variety of sources:
  – Email;
  – Web surfing;
  – Infected documents;
  – Exploits of "latent" Windows vulnerabilities.

✦ Malicious autorun.inf on usb memory sticks:
  – Windows domain policy to disable autorun and autoplay;
  – System can still be infected if the user clicks on the wrong file.

✦ Don't load "unknown" media into your system!

✦ Patch early & patch often!

Recent Incidents - Linux

✦ Linux Kernel vulnerabilities:

– Exploits of latent Linux Kernel vulnerabilities to compromise system;

– Typically require local access in order to launch;

– The author(s) of the Phalanx rootkit have been observed to "enhance" the rootkit to take advantage of newly disclosed Kernel vulnerabilities within hours of new Kernel releases.

✦ Patch early & patch often!

Recent Incidents – Mac OS

✦ "Typhoid Mary" associated with autorun.inf on usb memory stick.

✦ Don't load "unknown" media into your system!

✦ Patch early & patch often!

Recent Incidents – All OSes

✦ Copyright violations via peer-to-peer (P2P) networking (example: BitTorrent).

Recent Incidents – DOE Audit in 2009

✦ Systems not being administered per policy;

✦ Users and system administrators not responding appropriately to incidents;

✦ Passwords not meeting minimum complexity requirements;

✦ Passwords being written down;

✦ Doors not being locked after hours.

Recent Incidents - Other

✦ An individual paging FCIRT after business hours because they could not log into a system:

– They had not been granted access by the system administrator;

– They also wanted additional software to be installed on the system.

✦ Could this be a social engineering attack?

Recent Incidents – SL(F) 3

- ✦ Scientific Linux was "end of lifed" on 10-Oct-2010 (10/10/10).
  - – Security updates are no longer available.
  - – Warnings had been issued for over a year.
- ✦ If you **ABSOLUTELY NEED** to run SL(F) 3, then you must request and be granted an OS baseline exemption.
- ✦ Your request should list:
  - – The reason why you need to run SL(F) 3
  - – The "compensatory" controls that you will deploy.
  - – The expected duration of your exemption request.
- ✦ Even if you are granted an OS baseline exemption, if there is an incident associated with the system, it may be subject to immediate banning from the network!

FNAL Strategy

✦ Integrated Security Management
✦ Defense in Depth:
  – Perimeter Controls and auto blocking;
  – Mail gateway virus scanning;
  – Central Authentication:
    • Kerberos;
    • "Services Account" – Single account and password for various "application suites".
  – Major Applications with enhanced security concerns;
  – Minor Applications with enhanced security concerns;
  – Patching and configuration management;
  – Critical vulnerabilities;
  – Prompt response to computer security incidents (FCIRT);
  – Intelligent and informed user community.

Integrated Security Management

✦ Computer Security is not an add-on or something external, it is part and parcel of everything you do with computers (analogy with ES&H, and Quality Assurance);

✦ Not "one-size-fits-all", but appropriate for the needs and vulnerabilities of each system;

✦ In most cases, it is simply common sense + a little information and care;

✦ Each Division/Section or large experiment has a GCSC (General Computer Security Coordinator) who acts as liaison with the Computer Security Team in disseminating information and dealing with incidents; see **http://security.fnal.gov/** for an up to date list.

Perimeter Controls

✦ Certain protocols are blocked at the site border (email to anything other than lab mail servers; web to any but registered web servers; other frequently exploited services)

✦ Temporary (automatic) blocks are imposed on incoming or outgoing traffic that appears similar to hacking activity; these blocks are released when the activity ceases (things like MySpace and Skype will trigger autoblocker unless properly configured)

Central Authentication

✦ All use of lab computing services requires central authentication

✦ Avoid disclosure of passwords on the network

✦ No network services (logon or read/write ftp) visible on the general internet can be offered with out requiring strongest authentication, currently Kerberos (unless a formal exemption is applied for and granted)

✦ Kerberos provides a single sign in, minimizing use of multiple passwords for different systems

✦ Lab systems are constantly scanned for violations of this policy

"Services Account"

✦ Your "Services Account" provides a shared account password sign in for applications such as the Fermilab Service Desk, Fermilab Time and Labor Reporting(Kronos), Fermilab IMAP and Exchange Email, VPN.

✦ Over time, more and more applications will come under the "Services Account" umbrella.

Major Applications

- ✦ Defined as "critical to the mission of the Laboratory", i.e. disruption may have major impact on Laboratory operations;
  - – Most things do *not* fall in this category;

- ✦ Special (more stringent) rules & procedures apply; each MA has its own security plan with enhanced and compensatory security controls beyond the baseline security controls;

- ✦ You'll know if you're in this category.

Minor Applications

- ✦ Defined as "important to the mission of the Laboratory", i.e. disruption may have significant impact on Laboratory operations;
  - Most things do *not* fall in this category;

- ✦ Special (more stringent) rules & procedures apply; each Minor Application has its own security plan with enhanced and compensatory security controls beyond the baseline security controls;

- ✦ You'll know if you're in this category.

Grid Security Training

✦ If you are a system administrator:
  – of one or more systems that accept grid jobs (generally jobs that are authenticated by credentials other than standard Fermilab Kerberos credentials);
  – of one or more of the systems that provide support for the Fermi Grid infrastructure (such as GUMS and VOMS servers);
  – a developer of grid middleware software.

✦ Then, in addition to "Security Essentials for Fermilab System Administrators":
  – you require the training course entitled "Security Essentials for Grid System Administrators" which is available both in face to face sessions and online.

✦ If you are a user of grid computing resources, then:
  – you require the training course about PKI Authentication.
  – It would also be a good idea to take FermiGrid 201/202.

Patching and Configuration Management

✦ Baseline configurations exist for each major operating system (Windows, Linux, MAC);

✦ All systems must meet the baseline requirements and be regularly patched (in particular running an up-to-date supported version of the operating system) UNLESS:
  – A documented case is made as to why the older OS version cannot be upgraded;
  – Documentation exists to demonstrate that the system is patched and managed as securely as baseline systems;
  – Appropriate "compensatory controls" to mitigate the resultant risk are established on the system;
  – All non essential services (such as web servers) are turned off.

✦ You as a system administrator are responsible for configuration and patching!

Anti-Virus

✦ Baseline configurations for Windows and Mac OS require that the systems run laboratory managed anti-virus software;

✦ Linux systems with Windows file systems must also run anti-virus software;

✦ Anti-Virus software must be configured to report to the corresponding centrally managed anti-virus server and/or update console;

✦ You as a system administrator are responsible for configuration and updates!

✦ You are also responsible for responding to anti-virus alerts!

Central Logging

✦ System administrators are encouraged to configure their systems to send copies of the relevant system logs to clogger.fnal.gov;

Critical Vulnerabilities and Vulnerability Scanning

✦ Certain security vulnerabilities are declared critical when they are (or are about to) being actively exploited and represent a clear and present danger;

✦ Upon notification of a critical vulnerability, systems must be patched by a given date or they will be blocked from network access;

✦ This network block remains until remediation of the vulnerability is reported to the TISSUE security issue tracking system (as are blocks imposed for other security policy violations).

Anti-Virus Alerts & Automatic Blocking

✦ Certain anti-virus alerts that represent a clear and present danger will result in the system being automatically blocked from the network;

✦ Depending on the particular anti-virus alert, the system may require an immediate "wipe and reinstall";

✦ If the anti-virus alert does not require an immediate "wipe and reinstall", then the system will be:
  – Manually scanned via a bootable CD;
  – Any infection found removed;
  – And re-scanned via the bootable CD to verify that all infections have been completely removed;
  – If the infections are not completely removed then a "wipe and reinstall" will be performed.

✦ The network block will remain in effect until remediation of the anti-virus alert is reported to the TISSUE security issue tracking system.

Computer Security Incidents

✦ Mandatory incident reporting:
- Report all suspicious activity:
  - *If urgent* to FCC Helpdesk, x2345, 24x7;
  - *Or* to system manager (if immediately available);
  - Non-urgent to computer_security@fnal.gov;
- Incidents investigated by Fermi Computer Incident Response Team (FCIRT);
- *Not* to be discussed!

Fermi Computer Security Incident Response Team (FCIRT)

✦ Security experts drawn from throughout the lab

✦ Investigate ("triage") initial reports;

✦ Coordinate investigation overall;

✦ Work with local system managers;

✦ Call in technical experts;

✦ May take control of affected systems;

✦ Maintain confidentiality;

Prohibited Activities

- "Blatant disregard" of computer security:
  - First time warning, repeat offense disciplinary action;
- Unauthorized or malicious actions:
  - Damage of data, unauthorized use of accounts, denial of service, etc., are forbidden;
- Unethical behavior:
  - Same standards as for non-computer activities;
- Restricted central services:
  - May only be provided by Computing Division;
- Security & cracker tools:
  - Possession (& use) must be authorized;
- See http://security.fnal.gov/policies/cpolicy.html

Mandatory System Manager Registration

✦ System managers must be registered:
  – Go to http://security.fnal.gov and click on "verify your node registration" to see who is registered as sysadmin for your system;
  – See: http://www.miscomp.fnal.gov/sysadmindb to make changes in registration (you will need a KCA certificate).

Your role as a user and system administrator

✦ You have a special role as sysadmin of 3 or more systems, a major application, or a central server;

✦ Sysadmins are on the "front line" of computer security:

"Fermilab's continuing policy has been to put its first line of defense at the individual responsible for the data and the local system manager."

✦ Three roles for a sys admin:
  – System manager (configure system, remove unneeded services, apply patches promptly);
  – examples for users;
  – vigilant observers of system (and sometimes user) behavior.

✦ Sysadmins are expected to communicate computer security guidelines and policies to the users of systems they administer;

✦ Most important: know how to tell what services are running on your desktop, turn off those not needed, know where you are getting your patches from (FERMI domain, Patchlink, yum, Microsoft, …).

Role of sysadmins

✦ Manage your systems sensibly, remaining aware of computer security while conducting everyday business;

✦ Advise and help users;

✦ Keep your eyes open;

✦ Report potential incidents to FCIRT;

✦ Act on relevant bulletins.

Protecting Your Systems

✦ Most of the measures you'd take to protect system and data integrity against random hardware failures or user error are also effective against network attacks, viruses and other malicious code.

✦ The other basic measures are fairly simple:
  – Shut off services you don't need. They may be vulnerable to attack, attacks may be discovered at a later date, or they may require careful configuration to be secured;
  – Understand the services you do need. Configure them properly and keep up to date with patches;
  – Keep yourself informed about security issues with the OS and applications you use;
  – Don't trust your system logs, they are the first thing an attacker will modify if your system is compromised.
    • >>> Forward your system logs to clogger.fnal.gov <<<

Your role as a computer user

✦ Guard against malicious code in email
  – Don't open attachments unless you are sure they are safe
  – Don't trust who email is from
  – Updated and enabled virus signatures
✦ Guard against malicious code from web browsing
✦ Obey Central Authentication Policy (Kerberos / "Services Account")
  – Don't run network services (login or read write ftp) unless they demand Kerberos authentication
  – Treat your passwords as a sacred object (never expose it over the network)
✦ Promptly report potential computer security incidents
  – X2345 or computer_security@fnal.gov
  – Follow FCIRT instructions during incidents (especially about keeping infected machines off the network and preserving the status of an infected machine for expert investigation)

Other Computing Policy Issues

- ✦ Data backup
- ✦ Incidental use
- ✦ Privacy
- ✦ Offensive material
- ✦ Licensing

Data Backup Policy - Users

✦ Users (data owners) responsible for determining:

– What data requires protection;

– How destroyed data would be recovered, if needed;

– Coordinating backup plan w/ sysadmins;

  • or doing their own backups;

– If the backup is done for you it might be worth occasionally checking that:

  • The data is really being backed up!

  • You can really retrieve the data!

Incidental Computer Usage

✦ Fermilab policy permits some non business use of lab computers

✦ Guidelines are at
http://security.fnal.gov/ProperUse.htm

Activities to Avoid

✦ Large grey area, but certain activities are "over the line";

– Illegal;

– Prohibited by Lab or DOE policy;

– Embarrassment to the Laboratory;

– Interfere w/ performance of job;

– Consume excessive resources;

✦ Example: P2P (peer to peer) software like Skype and BitTorrent: not explicitly forbidden but very easy to misuse!

Privacy of Email and Files

- ✦ Fermilab normally respects the privacy of electronic files and email;
- ✦ Employees and users are required to do likewise;
- ✦ Certain exemptions for system managers and computer security response;
- ✦ All others *must* have Director(ate) approval;

Privacy of Email and Files

✦ May not use information in another person's files seen incidental to any activity (legitimate or not) for any purpose w/o either explicit permission of the owner or a "reasonable belief the file was meant to be accessed by others."

– Whether or not group/world accessible;

– "Group" files implicitly may be used by the group for the mission of the group;

Offensive Material on computers

- Many "computer security" complaints are not;
- Material in a computer is like material in a desk;
  - With respect to both privacy and appropriateness;
- This is a line management, not computer security, concern (except in egregious cases).

Software Licensing

✦ Fermilab is strongly committed to respecting intellectual property rights;

✦ Any use of unlicensed commercial software is a direct violation of lab policy.

Summary: User Responsibilities

✦ Appropriate use of computing resources;

✦ Prompt incident reporting;

✦ Proper Information handling (see Protecting Personal Information course);

✦ Know how your data is backed up;

✦ Receive computer security training;

✦ Respect privacy of electronic information;

Summary: System Admin Responsibilities

✦ System registration;

✦ Virus protection, patching and configuration management;

✦ Access control: telnet and ftp type services require kerberos authentication;

✦ Do not offer any of the restricted central services!

Questions?

- nightwatch@fnal.gov for questions about security policy
- Computer_security@fnal.gov for reporting security incident
- http://security.fnal.gov/